Declassified in Part - Sanitized Copy Approved for Release 2013/05/28 : CIA-RDP85M00364R000701140027-3

NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE
FORT GEORGE G. MEADE, MARYLAND 20755

Rec'd w/ltr
Executive Registry
83-0069
Reference C

Serial: N-1505-82
27 December 1982

7 JAN 1983

MEMORANDUM FOR THE DEPUTY DIRECTOR OF CENTRAL INTELLIGENCE

SUBJECT: Community Data Processing Support for Capabilities Programming and Budgeting (CPB)

1. Our staffs have completed their specification and evaluation efforts, as described in my memorandum of 15 March. They have produced a proposal which is within the congressional guidance for CPB processing support for the Intelligence Community (IC) Staff. This proposal is to use our Administrative Computer, on which we perform our CPB processing, and to use the software packages on this system to develop CPB support for the IC Staff.

2. Our staffs have defined a minimum set of requirements that will be met as the initial operating capability (IOC) of the system. The attached statement of requirements provides a detailed description of these requirements. In brief, the functions to be performed at IOC are:

a. Connect the NSA host system with communications to the IC Staff, the CIA, the DIA [redacted] 25X1

b. Provide an electronic mail capability between the users to support exchanges concerning congressional questions and their answers, for example.

c. Provide a capability to store and forward files, such as the Congressional Budget Justification Book narratives.

d. Connect existing word processing terminals to the system, if practicable.

e. Provide system access and data access security.

f. Provide a demonstration data base.

After IOC, the existing data base support for the IC Staff would be replaced on the Administrative Computer. The development of this support would be under the same data base system that we use for our CPB processing and would have compatibility of the two systems as a design goal.

DCI EXEC REG

~~FOR OFFICIAL USE ONLY~~

Declassified in Part - Sanitized Copy Approved for Release 2013/05/28 : CIA-RDP85M00364R000701140027-3

Declassified in Part - Sanitized Copy Approved for Release 2013/05/28 : CIA-RDP85M00364R000701140027-3

3. The delivery of the capabilities described above (items a. through f.) will require some three man years over a 12-month period, primarily to accomplish the communications work. NSA will provide the manpower to work communications for the host computer to the various agencies. Communications within each agency would be the responsibility of that agency. The development of the data base capability, to replace the existing IC Staff CPB data base system, will require some nine man years, over a 24-month period. Our computer organization will provide four man years of effort; our program and budget organization will provide one man year of effort; and the IC Staff will provide four man years of effort. Informal discussions with the staff have resulted in the identification of two persons who will work full time at NSA in the development of the data base system.

4. After the IOC system and the data base capability have been delivered, our computer organization will provide an additional four people full time for operations and software life-cycle support. The IC Staff will provide the personnel to do the development of any new applications software or enhancements to the delivered applications and to provide user support.

5. I trust this proposal meets with your agreement.

LINCOLN D. FAURER
Lieutenant General, USAF
Director NSA/Chief, CSS

Encl:
a/s

Declassified in Part - Sanitized Copy Approved for Release 2013/05/28 : CIA-RDP85M00364R000701140027-3

Declassified in Part - Sanitized Copy Approved for Release 2013/05/28 : CIA-RDP85M00364R000701140027-3

Capabilities Programming and Budgeting System

1. Introduction:

The basic requirement for an Intelligence Community Capabilities Programming and Budgeting (CPB) System was stated by the Deputy Director for Central Intelligence in his memorandum to General Faurer, dated 22 February 1982. His statement of the requirement is as follows:

> NFIP components will have electrical access to a Community computer, using, wherever possible, existing word processing terminals. The central computer will serve as a communications medium between the ICS and all components. In addition, the ICS and some components will use the Community computer to maintain and manipulate their detailed budget data. Other components may choose to use their in-house computers for data base maintenance and provide updates to the Community computer as required. Data and text will be merged to produce required displays using word processor stations--first as terminals to generate and retrieve numeric reports on the mainframes, and then as word processors to add the narrative discriptions. Combined displays will then be communicated with the ICS through the Community computer, edited as required during budget review, and ultimately form the basis for large portions of the Congressional Budget Justification Books (CBJBs). CBJB material will be communicated from the Community computer to the printing and Photography Division at CIA for photo composition and printing.

Discussions with representatives of the Intelligence Community Staff (ICS) have identified a subset of the overall requirement which represents the minimum essential requirement (MER) for an initial operating capability (IOC). The following paragraphs further define the overall IOC requirement. The MER requirements are divided into four subsets of requirement: functional requirements, security requirements, performance requirements and system requirements. Functional requirements are the requirements the user has for specific functions to be performed. Security requirements are the user's requirements for access to and protection of the system, the data on the system, and the functions of the system. Security requirements also include the physical security (TEMPEST) requirements for the hardware and terminals. Performance requirements are the user's requirements for the system's availability and responsiveness. System requirements are a function necessary to meet the user requirements defined under the three categories described above.

ENCLOSURE

Declassified in Part - Sanitized Copy Approved for Release 2013/05/28 : CIA-RDP85M00364R000701140027-3

Declassified in Part - Sanitized Copy Approved for Release 2013/05/28 : CIA-RDP85M00364R000701140027-3

2. IOC Requirements

The IOC CPB system requirements are as follows:

2.1. Functional Requirements

The functional requirements for the IOC CPB system are: for a word-processing function, supported by communications linking existing word-processing capabilities at the ICS, CIA, DIA, NSA, and Special Activities, Air Force with the community computer; an electronic mail function; a store and forward data function; and a prototype of these requirements follows.

2.1.1 Word-Processing Function

The fundamental word-processing requirement is to enable existing word-processing terminals at the NFIP components noted above to access the community computer. The actual word-processing function will be performed on the word-processing terminals with output to be made available to the community computer. The communications requirement to support this access is covered under system requirements.

While the community computer will not be expected to support a full word-processing function, it should be able to support the editing of sequential files.

2.1.2. Electronic Mail Function

The electronic mail function is intended to supply the users with a means of communicating with each other via the system. The specific functions to be supported are:

a. Exchange informal correspondence and notes with other users.

b. Exchange formal correspondence with other users.

c. Exchange congressional questions and answers with other users.

d. Retrieve mail by subject.

e. Edit mail messages before releasing them to other users.

f. Retain mail messages for a period of time after receipt.

Declassified in Part - Sanitized Copy Approved for Release 2013/05/28 : CIA-RDP85M00364R000701140027-3

Declassified in Part - Sanitized Copy Approved for Release 2013/05/28 : CIA-RDP85M00364R000701140027-3

g. Submit mail messages prepared on a word-processing terminal for inclusion in the mail system.

h. Archive congressional questions and answers and formal correspondence included in the mail system.

2.1.3. Store and Forward Function

The store and forward function provides the ability to transfer files between the user's word processors or in-house computers and the community computer. This function will be used for the following purposes:

a. The transfer to and storage on the community computer of files generated on the user's word processors. This will include narrative files supporting budget submissions and CBJB narrative.

b. The transfer of files stored on the community computer to the user's word processors. This also will include narrative files supporting budget submissions and CBJB narrative.

c. The transfer and storage of individual updates to the user's word processors. This also will include narrative files supporting budget submissions and CBJB narrative.

d. The transfer and storage of bulk updates to the ICS CPB data base. These updates will normally have been generated on the user's in-house computer.

e. Files transferred and stored on the community computer must be available in hard or soft copy to the ICS.

2.1.4. Prototype Data Base Function

The prototype data base requirements is, as far as is practicable, to be able to demonstrate some of the CPB Data Base features that will be required for the data-base support of the system. The capabilities to be demonstrated, in relative priority, are as follows:

a. to retrieve data using predefined queries,

b. to make ad hoc (interactive and batch) retrievals of data,

c. to apply updates (interactive and batch) against the data base,

Declassified in Part - Sanitized Copy Approved for Release 2013/05/28 : CIA-RDP85M00364R000701140027-3

Declassified in Part - Sanitized Copy Approved for Release 2013/05/28 : CIA-RDP85M00364R000701140027-3

d. to restrict access to the data base and to restrict access to specific data within the data base,

e. to protect the data integrity of the data base,

f. to use formatted screens for ease of user data entry and access to the data base,

g. to use data-base administration tools.

2.2. Security Requirements

The basic security requirements are as follows:

2.2.1. TEMPEST

The hardware and terminals will need to meet the appropriate TEMPEST criteria.

2.2.2. System Access

The host system on which the CPB system resides must support control of user access to the system. This will involve a means of identifying users that are authorized to access the system and of authenticating them at the time they attempt to gain access. This access mechanism also must be able to control access to specific capabilities on the system, such as access to the CPB system.

2.2.3. Data Access

The system must support control of user access to data. This includes access to data base files, to sequential files that are not physically part of the data base, and to mail files. Within the Capabilities Programming and Budgeting Data Base, access to the data must also be controlled at the record level.

The file access levels of control are: access not allowed, read only access allowed, read and write access allowed. The system must allow the owner of a file to establish the access level of other users. The data base administrator is considered the owner of the CPB Data Base and will establish the access level for all users of the data base. The owner of a sequential file will establish the access level for other users of that file. The system default access for all files must be no access allowed, to ensure that access to a file will be determined by the file owner. The only access to the data not controlled by the data-base adminstrator for the CPB Data Base or by the owner of a sequential file will be that necessary to ensure the integrity of the system; that is, access to the data will be available to the system administrator and to the security administrator, as a matter of necessity.

Declassified in Part - Sanitized Copy Approved for Release 2013/05/28 : CIA-RDP85M00364R000701140027-3

Declassified in Part - Sanitized Copy Approved for Release 2013/05/28 : CIA-RDP85M00364R000701140027-3

For those users authorized access to the CPB Data Base, access control at the record level will determine whether a user is authorized access to all or only some of the records in the data base. This level of access control will be based on an individual's clearance level and need to know.

2.2.4. Security Audit Trail

The system must support the logging of an audit trail to record attempts to access the system and attempts to access files. The DBMS which support the CPB Data Base should support the logging of an audit trail to record accesses to the data base and its data. Failure to provide the proper authentication for the attempted level of access, (system access, file access or data base access) also should be recorded.

2.3. Performance Requirements

The performance requirements establish the criteria for system availability, system responsiveness, and for the time to perform various system functions, such as recover/restore a file. The requirements are:

2.3.1. Availability

a. The system must be available for interactive use from 0630 to 1830, Monday through Saturday, during the months of February through August.

b. The system must be available for interactive use from 0630 through 2130, Sunday through Saturday, during the months of September through January.

c. Overall availability of the system (hardware and software) should be 95 percent.

d. The system must be available for overnight batch updates to the data base.

2.3.2. Response Time

a. The system should respond within 2 seconds to command-level instructions, edit session instructions, etc.

b. The system should respond within 10 seconds to data-base actions.

(Since this system operates on a large multiple use system, these response times may not always be satisfied.)

Declassified in Part - Sanitized Copy Approved for Release 2013/05/28 : CIA-RDP85M00364R000701140027-3

Declassified in Part - Sanitized Copy Approved for Release 2013/05/28 : CIA-RDP85M00364R000701140027-3

2.3.3. Throughput

Batch updates to the data base should be accomplished within 1 hour. At IOC there will be no other batch processing with any specific throughput requirement.

2.3.4. Recover/Restore Files

Recovery/restoration of files, when required, should be accomplished with 3 hours from the time the file becomes unavailable.

2.4. System Requirements

2.4.1. Communications Requirements

At IOC the system will need communications to support both interactive and RJE access for remote terminals, both CRTs and printers. The remote terminals will be located at the IC Staff, NSA, CIA, DIA (Pentagon), and the Special Activities, Air Force (Pentagon). For all users but the IC Staff, the interactive support should be via lines with a 9.6KB speed. The terminals to be connected are Xerox 860 terminals at NSA, DIA and the Special Activities, Air Force (SPAF), and either NBI or WANG terminals at the IC Staff and CIA. Both types of terminals should be interfaced via an emulator to operate in 3270 mode. Initially there will be no more then 25 terminals to be connected to the system.

2.4.2. Hardware Requirements

The CPB system will reside on the NSA Administrative system, an IBM 3081. The hardware requirements for the IOC system are as follows:

a. The terminal requirement is to be met by existing word-processing terminals, as far as is practicable. The terminals, therefore, must be capable of interfacing to the IBM mainframe.

b. The hardware configuration must be capable of supporting 20-25 terminals at IOC.

c. The system should have at least 5 billion bytes of real DASD available for user files.

d. The system should be able to support simultaneous journaling and output on tape drives.

e. The system configuration should be suitable for ease of switching to a back-up system.

Declassified in Part - Sanitized Copy Approved for Release 2013/05/28 : CIA-RDP85M00364R000701140027-3

Declassified in Part - Sanitized Copy Approved for Release 2013/05/28 : CIA-RDP85M00364R000701140027-3

2.4.3. Software Requirements

The CPB system will use software packages that are already in use on the Administrative system. No requirement for other software packages exists for the IOC system.

2.4.4. Back-Up Requirements

a. System back-up
The CPB system requires a back-up capability for any period of system unavailability that is expected to exceed eight hours. The back up capability must be able to meet all of the CPB functional and security requirements. It is recognized that the back-up capability may not be able to meet all of the CPB performance requirements.

b. File back-up
Data base files will need to be backed up once a day, for system back-up purposes. If the DBMS provides automatic recovery, no further back-up of the data base files will be necessary. If there is to be no automatic recovery by the DBMS, the data base files will need to be backed up twice a day. Sequential files related to the data base and all mail files will need to be backed up once a day.
The daily back-up of files should be done out of normal operating hours (see Availability Requirements, above). If the data base files are to be backed up twice a day, the second back-up should be done during the operating day, at a point approximately midway between the beginning and ending of the operating day, to ensure that data base file problems do not affect more than half a day's work.

2.4.5. File Retention On-line

a. Data base files for budget years that no longer need to be two budget years immediately preceding the budget year being built will need to be on-line. In addition, "snap shots" of the data base will be taken at various key points in the budget cycle. These "snap shots" for the budget year and the preceding two years will also need to be on-line. Data for the two years preceding the budget year at IOC will need to be converted from the previous format to the CPB data base format.

Declassified in Part - Sanitized Copy Approved for Release 2013/05/28 : CIA-RDP85M00364R000701140027-3

Declassified in Part - Sanitized Copy Approved for Release 2013/05/28 : CIA-RDP85M00364R000701140027-3

b. Sequential files which store budget submission and CBJB narratives should be retained on-line in the same fashion as the CPB data base. Personnally owned sequential files should be subject to automatic deletion after a period of time or period of disuse.

c. Mail files will remain on-line in accordance with the procedures established by the Data Base Administrator.

2.4.6. File Retention Off-line

a. Data base files for budget years that no longer need to be on-line will be archived to tape for indefinite retention. The data base administrator will be responsible for invoking the archival procedure for the CPB data base.

b. Sequential files containing CBJB narrative or the narrative accompanying program budget submissions will be archived to tape for indefinite retention. The data base administrator will be responsible for invoking the archival procedure for these sequential files.

c. Congressional questions and answers and formal correspondence that no longer need to be on-line will be archived to tape for indefinite retention. The owner of these mail files will be responsible for staging them from the mail system. Periodically mail files so staged will be archived to tape.

2.4.7. Recovery Requirements

In addition to standard system recovery procedures, the system operators will be required to implement recovery procedures that will be defined during implementation planning. These procedures will cover any automatic and/or manual data base recovery and the recovery of sequential and mail files. AT IOC there will be no requirement for automatic recovery other than that identified for the data-base management system.

2.4.3. Support Requirements

a. The CPB system requires that configuration management procedures be adopted to cover system (hardware and software) changes, application software changes, changes to the data base, and the validation and handling of new requirements. These procedures will be in accordance with the management plan that will be defined during the implementation planning.

Declassified in Part - Sanitized Copy Approved for Release 2013/05/28 : CIA-RDP85M00364R000701140027-3

Declassified in Part - Sanitized Copy Approved for Release 2013/05/28 : CIA-RDP85M00364R000701140027-3

b. The CPB system requires that system administration functions, such as space management and the providing of systems information to users, be available.

c. The CPB system requires that a Data Base Administrator (DBA) be named to control the CPB Data Base. The DBA will be a member of the IC Staff data processing staff. He will be responsible for granting access to the data base, establishing security levels within the data base, overseeing the integrity of the data base, performing various data-base functions, controlling the data dictionary, and participating in any change control board governing the CPB Data Base. The DBA will also be responsible for determining standards and establishing procedures for sequential and mail files.

d. The CPB system requires that a system security administrator be named to control access to the system, data base and files. The system security administrator will be responsible for maintaining all password files and will be the ultimate authority for security matters concerning the CPB system.

Declassified in Part - Sanitized Copy Approved for Release 2013/05/28 : CIA-RDP85M00364R000701140027-3